Trusted Web におけるガバナンスの構築に関する考え方

目次

1.　Trusted Web 実現におけるガバナンスによるトラスト向上の必要性

(1). Trusted Web が目指す世界観

1.　「インターネット上ではあなたが犬だと誰も知らない」という”The New Yorker”の風刺画[1]にあるように、インターネットのプロトコルで実現される匿名性によるデジタル・アイデンティティの信頼性やプライバシーに関する課題が顕在化している。

2.　こうした中で、Trusted Web は、デジタル社会における様々な社会活動に対応するトラストの仕組みをつくり、多様な主体による新しい価値の創出を実現することを目的として、データの「出し手」が相手に開示するデータをコントロールすることを可能にし、データのやり取りにおける条件設定に関する合意の仕組みも取り入れつつ、相手から提供されるデータや合意の履行について検証（verify）できる領域を拡大し、これまで事実を確認せずに信頼していた領域を縮小できる新しいトラストの枠組みを構築するイニシアティブとして、推進されてきているものである。これにより、相手先が期待したとおりに振る舞うと信じる度合い、すなわち、トラストを高めることを目指すものである。

　特に、ユーザは、デジタル・サービスを利用する際に、提供元をどの程度トラストできるかを考慮しているが、現在、「事実を確認せず、デジタル・サービスの提供元を盲目的に信頼せざるを得ない」状況である。このため、盲目的に信頼せざるを得ない部分を減らすには、検証可能な部分を増やす必要がある。

[1] Peter Steiner, “On the Internet, nobody knows you're a dog” The New Yorker, 5, July 1993.

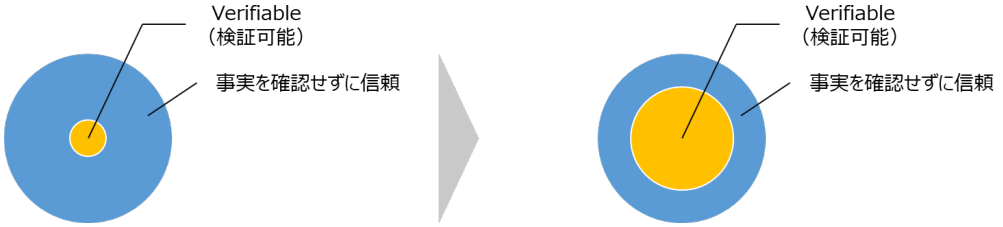

図 1. Verifiable(検証可能)な部分の拡大によるトラストの向上

(2). Trusted Web におけるガバナンスの必要性について

3. 検証（verify）できる領域を拡大する上では、技術的にはデジタル署名技術の活用や、プロトコル、データフォーマットの活用が考えられる。しかしながら、ユーザが安心してデジタル・サービスを利用するには、こうした技術の活用に加え、そのデジタル・サービスが、特定の技術プロファイルや特定のルール、法令に従った状態で運用されており（ガバナンスが効いている）、それが観測[2]できることが重要である。

4. この際、上記の Trusted Web が目指す世界観を、データのやり取りを行うコミュニティにおいて実現していく上では、例えば、
   - どの部分を検証可能とするか、どの部分を事実を確認せずに信頼することとするか、
   - 検証可能とする領域において、どのような技術プロファイルを活用するか、
   - どのような法令やルールに従うこととするか、
   - どのような形で、これらの技術プロファイルや法令、ルールに従った状態で運用がなされるべきか、

   といったことについて、コミュニティにおいて関係するステークホルダが一定の合意を図り、それに従った運用がなされることが効果的な場合がある。

5. このような、Trusted Web の実現を目指すコミュニティにおける関係するステークホルダ間の合意や決め事、運用方針等を、Trusted Web を具現化する上でのトラストフレームワークと位置づけることとする。

6. 欧州における eIDAS 規制や米国 NIST SP800-63 が政府調達に活用される場合のようにエンフォースメントを前提としたトラストフレームワークもあるが、Trusted Web を具現化する上でのトラストフレームワークでは、そうでないものも含めて定義している。

(3). 用語定義

7. 以下の通り、Trusted Web のガバナンスにおいて用語を整理している。

---

[2] 「観測できる」とは、必要なときに実施しようと思えば、いつでも検証可能な状態（検証に必要な処理が公開されている、あるいは適切なステークホルダが検証可能である等）であり、その上で、どこまで検証を行うかは、コストとリスクを踏まえて決定される。

表 1. 用語定義

用語	説明
トラストフレームワーク (Trust Framework)	Trusted Web を具現化する上でのトラストフレームワークとは、「Trusted Web の実現を目指すコミュニティにおける関係するステークホルダ間の合意や決め事、運用方針等（どの部分を検証可能とするか、どの部分を事実を確認せずに信頼することとするか、検証可能とする領域において、どのような技術プロファイルを活用するか、どのような法令やルールに従うこととするか、どのような形で、これらの技術プロファイルや法令、ルールに従った状態で運用がなされるべきか等）」を指す。（以下、本ドキュメントにおける「トラストフレームワーク」は、上記の Trusted Web を具現化する上でのトラストフレームワークを指す。）[3] なお、トラストフレームワークは、運用規則、スキーム規則、運用方針などの仕様、規則、協定の集合（エコシステム内においてトラストフレームワークに準拠していることを示すことができる認証プロセスや、準拠状態を維持・監査するための、ガバナンスや監査機関を含むこともある。[4]）を指すことが多いが、ここでは、それとは異なっていることに留意する必要がある。
信頼	事実の確認をしない状態で、相手先が期待したとおりに振る舞うと信じる度合い

2. Trusted Web ホワイトペーパーver.3.0 で論じたガバナンスの考え方への当てはめ

(1). Trusted Web ホワイトペーパーver.3.0 で論じたガバナンスの考え方への当てはめ

8. 上記で述べた Trusted Web を具現化する上でのトラストフレームワークは、ホワイトペーパーver.3.0 におけるガバナンスの全体像における整理に従えば、第１階層である Trusted Web の概念を踏まえ、各コミュニティにおいて第２階層、第３階層で活用されるべき、トラストフレームワークと位置付けられる。

[3] ここでの「Trusted Web を具現化する上でのトラストフレームワーク」はホワイトペーパーver.3.0 実装編のアーキテクチャにおけるコミュニティポリシーに相当するものである。

[4] 出典：Open Identity Exchange “A Guide to Trust Frameworks for Smart Digital ID”。

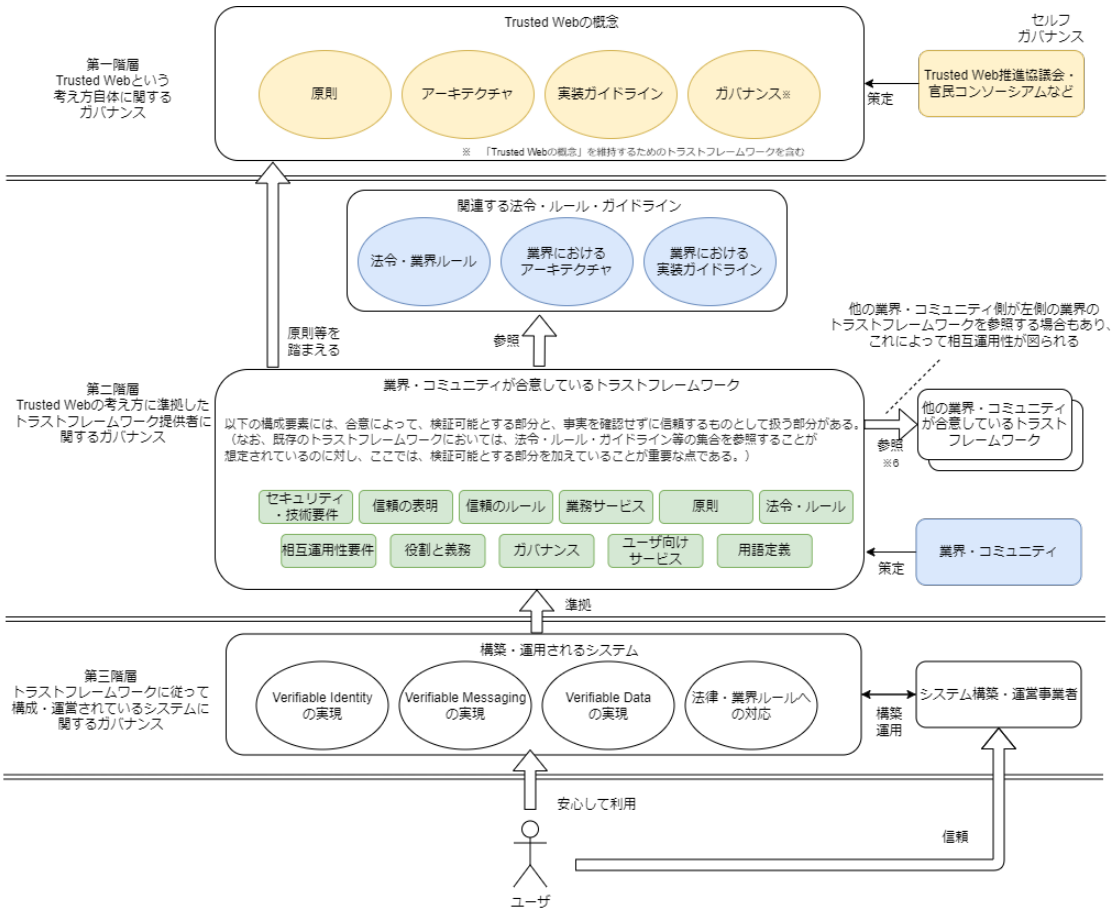

図 2. Trusted Web におけるガバナンスの全体像 [5]

9. 第２階層、第３階層において各コミュニティがトラストフレームワークに合意し、運用を行っていく上では、第１階層で示されている Trusted Web の概念を踏まえたものであることに加え、第１階層で提起されている原則[7]についても留意するべき事項がある。

10. 具体的には、原則の一つとして掲げられている「マルチステークホルダによるガバナンス」（マルチステークホルダがガバナンスに関与し、責任を明確化し、問題が発生した際に原因究明ができる）を踏まえれば、トラストフレームワークは、コミュニティにおけるステークホルダが合意する事項と捉えることができる。この際、このトラストフレームワークにおいては、後述するトラストフレームワークで検討する項目の全てを含める必要はなく、コミュニティにおいて必要とされるトラストフレームワークの役割やそれに伴うトラストフレームワークの品質（有効性や強度）に応じて自由度をもって考

[5] タスクフォースでの議論を踏まえ、理解の一助となるようにホワイトペーパーver.3.0 の図に一部補足を加えている。
[6] 法令によって、他の業界・コミュニティのトラストフレームワークを参照することを認めているケースもある。
[7] ホワイトペーパーver.3.0

えることができるものである。

11. また、Trusted Web の原則の一つとして「相互運用性」が掲げられているところ、コミュニティにおいてガバナンスを機能させる上では、他のコミュニティのトラストフレームにおける規約や仕様を参照することがあり得る。すなわち、様々なトラストフレームワークにおける規約や仕様を参照することで全体のガバナンスが構築されるため、個々のコミュニティにおいてはシステムアーキテクチャに加え、コミュニティにおいて採用することに合意する技術プロファイルや法令・ルールを含めたトラストフレームワークやガバナンスについても、相互運用性を意識することが重要である。

さらに、原則において「柔軟性」、「更改容易性・拡張性」が掲げられているところ、拡張可能なシステムアーキテクチャとするため、構成部品が疎結合で構成される柔軟性も留意する必要がある。

(2). 具体的な事例（運転免許証を身分証明書として使うシーン）

12. 以上で整理したことを踏まえ、一つのコミュニティが他のコミュニティのトラストフレームワークを参照する具体的な事例として、図 3 に示す運転免許証を金融機関に提示する身分証明書として使うシーンを考える。

13. 運転免許証は都道府県の公安委員会を発行者として、交付を受けた者に運転能力があることを保証すると同時に、券面に氏名や生年月日、住所が記載される。運転免許証の発行業務における決め事をトラストフレームワークと考えると、検証者（例えば、警察官）は運転免許証を提示した者が運転能力を保持することを検証することができる。

14. その際、氏名や生年月日、住所に関しては、運転免許証の初回の発行の際に市町村から発行される住民票を提出することで確認されている。これは、運転免許証のトラストフレームワークが住民票におけるトラストフレームワークを参照していると整理することができる。

15. その上で、運転免許証には、氏名や生年月日、住所が記載されているため、運転免許証のトラストフレームワークの本来の目的ではない、金融機関に提示する身分証明書として使う場合が存在する。ただし、運転免許証は、例えば、市町村に届け出る住所変更があった際に、現状においては、運転免許証の所持者が住所変更とは別に、記載事項の変更を公安委員会に届ける必要があるため、最新の住所ではない可能性がある。

16. このため、金融機関が運転免許証を身分証明書として用いるときに、運転免許証に記載された住所を金融機関側として受け入れることができない場合は、公共料金の領収書などを用いて追加で検証をすることで、より信じること（トラストを高める）ができる。

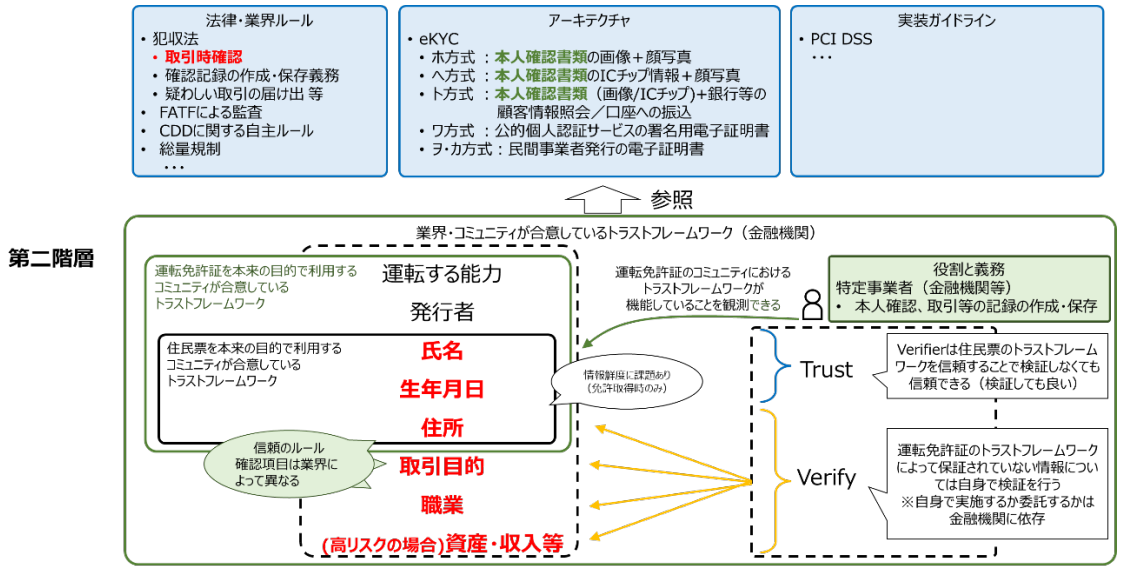

図 3. トラストフレームワークの外からの参照関係

（金融機関における免許証を使った身元確認を例に単純化）

3. ガバナンスの構造を踏まえたトラストフレームワークの策定方法の提案

17. 前述の図２に示す通り、第１階層においては、Trusted Web の概念を具現化するための原則等を示しており、ホワイトペーパーver.3.0 では、第２階層、第３階層で検討すべきトラストフレームワークの構成要素（以下の表 2）を示している。

18. なお、検討すべきトラストフレームワークの構成要素においては、Trustd Web の原則の全てを準拠する必要はなく、コミュニティにおいて必要とされるトラストフレームワークの役割やそれに伴うトラストフレームワークの品質（有効性や強度）に応じて自由度をもって考えることができる。

表 2. トラストフレームワークの構成要素と Trusted Web の具現化時に考慮すべきこと

構成要素[8]	Trusted Web の具現化時に考慮すべきこと（例）
用語定義（Glossary）	-
原則（Principles）	Trusted Web の原則に準拠すること
信頼の表明（Trust Mark）	仮にユーザ等に向けて Trusted Web に準拠したトラストフレームワークであることを表明する場合は原則の遵守状況のモニタリングの必要性などについて検討すること
役割と義務（Roles and Obligations）	Trusted Web の原則の遵守を義務として定義すること
ガバナンス（Governance）	Trusted Web のガバナンスの概念を踏襲すること（マルチステークホルダ等）
信頼のルール（Trust Rules）	Trusted Web の原則に則り構成されるエンティティを信頼すること
ユーザ向けサービス	Trusted Web の原則に則り構成されること（検証可能性、

[8] OIX のトラストフレームワーク構成要素より引用（https://openidentityexchange.org/a-guide-to-trust-frameworks-for-smart-digital-id?page=digital-identity-trust-framework）

（User Services）	透明性など）
業務サービス （Relying Party Services）	同上
法令・ルール （General and Legal Rules）	参照すべき法令・ルールを特定すること
セキュリティ・技術要件 （Security and Technical Requirements）	検証可能性を担保できる技術を採用すること。特定の事業者によってのみ策定された技術ではなく、標準として広く受け入れられている技術を採用すること。
相互運用性要件 （Interoperability Requirements）	標準として広く受け入れられている技術を採用し、必要に応じてエコシステムの拡大を容易に行うことが可能なこと

19. 一方で、実際にトラストフレームワークを策定していく際には、コミュニティにおいて合意していく事項をベースに検討を進めていくことが容易と考えられる。このため、合意していく事項として、大カテゴリとして「技術プロファイル」と「法令・ルール」としている。（図 4 参照）

20. 技術プロファイルを詳細化すると、証明書やデータのやり取りにおける「フォーマット」や、ユーザ自身が、自らに関連するデータのコントロールや鍵関連情報・証明書のライフサイクル管理を行うための「プロトコル」、暗号技術をはじめとした「署名方式」等が中カテゴリとして考えられる。

21. 法令・ルールを詳細化すると、ドキュメントに対する改ざん検知や署名者の識別機能に関する電子署名法といった「法令」、サプライチェーンにおける安全で信頼性の高い実装を目指した Catena-X 等の「業界・慣習法」、医療に関連した情報システムを対象とした３省２ガイドライン等の「ガイドライン・ルール」等が中カテゴリとして考えられる。

22. これらの大カテゴリ、中カテゴリについて、コミュニティの目的等を踏まえて、必要な項目について選定することによって表 2 の構成要素に対応していくこととなる。

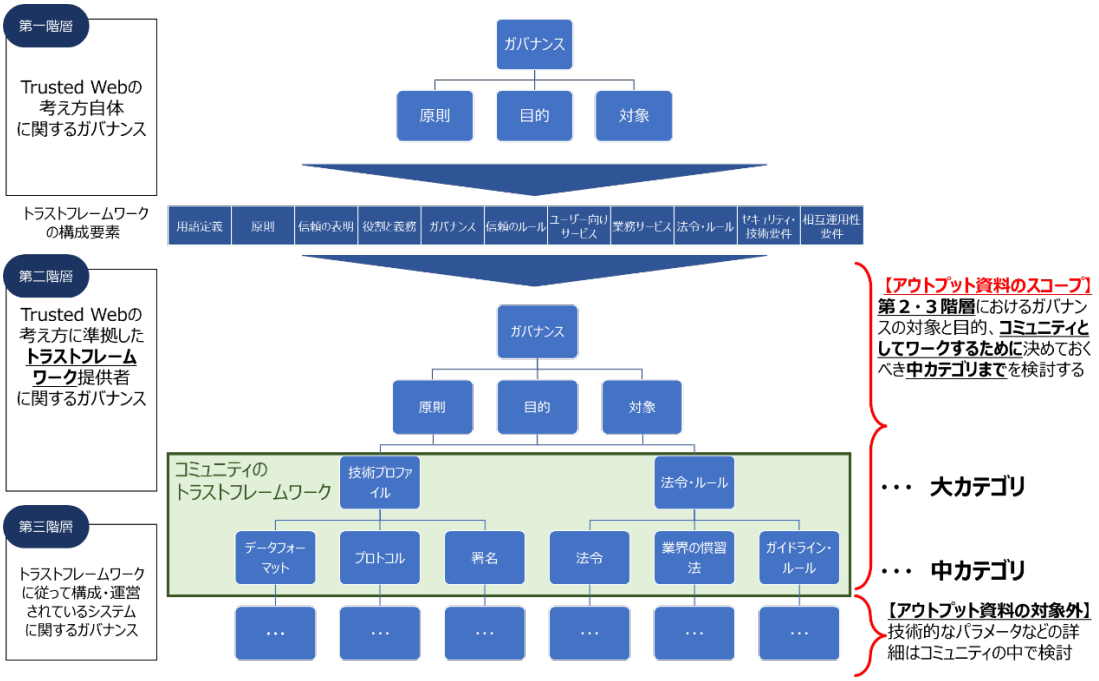

図 4. ガバナンスの階層における全体像

23. 表 3 は、以上の考え方を踏まえて、各コミュニティでトラストフレームワークを策定する際の参考として示したものである。表 3 にあるように、各項目の検討に当たっては、記載されている「考慮すべき事項」等を念頭に置くことで、検討すべき大枠を把握することができる。また、既存の法令・ルール等を参照してトラストフレームワークを策定することができる。

24. このように、個々の項目を選定しつつ、表 3 にあるように、各構成要素との対応関係を整理していくことができる。

25. 表 4 では、具体的なユースケースの事例として、移動支援や高齢者見守りなどの分野で生活者同士のマッチングによる手助けを促進する共助アプリにおいて、共助アプリ間で連携できることを目的に策定したトラストフレームワークについて紹介する。

26. その他、2023 年度に実施した実証事業の各ユースケースにおいても、表 5 に記載の通り、様々な法令・ルール、ガイドライン、規格・技術標準をベンチマークとしている。

表 3. トラストフレームワークにおける項目と考慮すべき事項等について

大カテゴリ	中カテゴリ	考慮すべき事項の例	関係エンティティ	構成要素との対応
技術	データ フォーマット	一貫したフォーマット（例 VC 等）	事業者	セキュリティ・技術要件 相互運用性要件
		属性情報の根拠情報	国際標準機関、政府	
		データモデル（例:vc-edu 等）		
	プロトコル	データ最小化、選択的情報開示	事業者、システム	信頼のルール
		セキュア領域のデータ管理	事業者、システム	ユーザサービス
		鍵とクレデンシャルのライフサイクル管理	事業者、システム	信頼のルール
	署名方式	暗号技術（CRYPTREC、BBS 等）	システム	セキュリティ・技術要件
法令・ ルール	法令	犯収法、電子署名法、個情法等	政府、事業者	法令・ルール
	業界・慣習法	データ管理（例:ChemSHERPA、GDPR 等）	政府、事業者	ユーザサービス
		アクセス管理	事業者、システム	業務サービス
	ガイドライン・ルール	プライバシー（名寄せ防止等）	ユーザ、政府、事業者、国際標準機関、システム	セキュリティ・技術要件
		セキュリティ（発行者の特定、改ざん検知等）		
		不正管理（3 省 2 ガイドライン等）		

表 4. トラストフレームワークにおける項目と共助アプリにおける検討事項

大カテゴリ	中カテゴリ	検討事項	構成要素との対応
技術	データフォーマット	★共助実績証明書に関する方針、スキーマ管理	セキュリティ・技術要件
	プロトコル	★通信プロトコルと標準規格の管理方針	信頼のルール
		★証明書発行に関する方針	ユーザ向けサービス
		★クレデンシャルの有効期限・失効に関する方針	信頼のルール
	署名方式	★暗号技術の活用方針	セキュリティ・技術要件
法令・ルール	法令	ー	法令・ルール
	業界・慣習法	シェアリングエコノミープラットフォーマに対する一般的な信頼性と安全性要件	ユーザ向けサービス
	ガイドライン・ルール	★プライバシーポリシーの策定	セキュリティ・技術要件
		★ガバナンス実行に関するポリシー	

★：共助トラストフレームワークとして策定

表 5. ユースケース実証事業において調査分析が行われた法令・ルール、技術プロファイル等

No.	代表機関	一般法規制・ルール	業界法規制・ガイドライン	規格・技術標準	業界団体・自主規制	サービス・個社取組
1	DataSign	•GDPR •eIDAS2.0	–	•OpenID Foundation •Matrix.org Foundation •Open Wallet Foundation	–	•EUデジタルアイデンティティウォレット
2	DNP	–	–	•ISO/TS 42501 •OpenID Foundation •Open Identity Exchange •Hyperledger Project	•シェアリングエコノミー協会	•Turing Space •Hyperledger Indyを活用した事例
3	IGS	•ベトナム個人情報規制	•ESCO基準 •EQF	–	–	–
4	富士通Japan	–	•厚生労働省策定キャリアマップ	–	•研究基盤協議会 •大学の各種規定	–
5	PitPa	•ネパール関連規制 •ネパール政府	–	•W3C •Open Identity Exchange	–	–
6	みずほR&T	–	•ELV指令 •RoHS指令 •TSCA •REACH規則 •SCIPデータベース	•ISO/IEC82474 •ISO/TC323 PCDS	•IMDSコミュニティ •MOBI •Gaia X、Catena-X •アーティクルマネジメント推進協議会 (chemSHERPA) •IPA DADC(ウラノスエコシステム)	•Hyperledger Fabricを活用した事例 (三井化学、Chemchain、TradeWaltz、 Circulor) •Cordaを活用した事例 (SBI Traceability、axedras)等 •他事例(SEMI)
7	SBIホールディングス	•eIDAS •電子署名法 •(eシールに係る検討)	–	•ISO/TC292 •ISO/IEC 17065 •ETSI EN 319 403 •NIST SP800-63-4 •W3C Credential Community Group	•一般社団法人　沖縄オープンラボラトリ •インターネット協会OIC BRPコンソーシアム •IPA DADC(ウラノスエコシステム)	•JIPDECトラステッド・サービス登録(認証局)
8	シミック	•GDPR •21 CFR Part11	•HIPAA •Digital Health Technologies(DHT) for Remote Data Acquisition in Clinical Investigations	–	•PHRサービス事業協会	•ORPHE
9	ORPHE	•個人情報保護法	•ALCOA原則 •次世代医療基盤法 •経産省_医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン	–	•一般社団法人PHR普及推進協議会	•シミック •Patients Know Best •Intuit Mint 等
10	電通総研	•eIDAS2.0	•犯罪収益移転防止法 •金融規制	•GAIN PoCプロジェクト •OpenID Foundation •ISO/IEC 27017/27001	–	–
11	JISA	•eIDAS2.0 •インドにおけるアカウントアグリゲーターフレームワーク	•各種省庁の補助金事務にかかるガイドライン	–	–	•EBSI-VECTORプロジェクトにおける法人ウォレット •GビズID •国税庁納税情報の添付自動化の仕組み
12	OP技術研究組合	–	–	•EV SSL規格 •Open Graph Protocol •JOURNALISM TRUST INITIATIVE •ads.txt	•Coalition for Content Provenance and Authenticity (C2PA) •JIQDAQ •Trustworthy Accountability Group	•NewsGuard

4. トラストフレームワークを踏まえたコミュニティ内、コミュニティ間のデータのやり取り

27. トラストフレームワークは、どの部分を検証可能とするか、どの部分を事実を確認せずに信頼することとするか等について、コミュニティにおいて関係するステークホルダ間で一定の合意を図る上で有効な手段である。

28. コミュニティ内でのデータのやり取りが最も基本的なユースケースとなり、コミュニティ内でトラストフレームワークの合意をするアプローチが重要となる。

29. 一方で、業界横断や越境のような異なるコミュニティ間でデータのやり取りをする場合は、各コミュニティ内で合意されたトラストフレームワークは、相手先のコミュニティとは合意されていないので、そのトラストフレームワークが有効に機能していること（ガバナンスが機能していること）をコミュニティの外から観測できる必要がある。

30. この際、コミュニティ間でのデータのやり取りが Trusted Web の原則で掲げられている「柔軟性」に従い、効率的にスケールしていくためには、どのようにコミュニティの外からトラストフレームワークを観測可能とするかが重要となる。

31. 例えば、DIF[9]などで行われているガバナンスが効いた状態をマシンリーダブルにするといった方法等が考えられる。

32. コミュニティ内、コミュニティ間におけるデータのやり取りは、以下の４つのパターンに類型化できる。

(1). コミュニティ内でやり取りする場合

(2). コミュニティ間でやり取りする場合

（ア）共通して参照するトラストフレームワークのトラストリストを信頼することでやり取りする場合

（イ）共通して参照するトラストフレームワークの決め事に準拠した（ただし、そのトラストリストには依拠しない）トラストフレームワークを採用するコミュニティ間でやり取りする場合

（ウ）共通して参照するトラストフレームワークがない中でコミュニティ間でやり取りする場合

33. なお、それぞれのステークホルダがデータのやり取りに関するトラストを構築しようとする際に、例えば、どの範囲の関連するステークホルダを取り込んだコミュニティを形成するかについては、自らが主体的にガバナンスに関与する範囲[10]をどのようにするかといった判断に基づいて考察することが必要となる場合もある。

---

[9] Credential Trust Establishment (identity.foundation)

[10] その他、トラストリストや対象とするデータ、対象とするデータにおける情報鮮度を含めた Verifiable な範囲における相手先コミュニティの差異も考えられる。

34.　例えば、ある事業者が、関連する事業者との間で信頼あるデータのやり取りを実現しようとする際に、既存のコミュニティに参加する場合はトラストフレームワークにおける決め事に関する意思決定等に実質的に関与できるかどうかが重要な判断要素となりうる。一方で、既存のコミュニティの外に別のコミュニティを形成することも可能であるが、その場合、既存のコミュニティにおけるガバナンスに対しては、外から観測するのみとなる。この場合、既存のコミュニティとの間で共通して参照するトラストフレームワークを持つこともできるが、そのあり方に関して、コミュニティ間で、合意できる範囲やトラストリストの運用について、追加での検討が必要となる。

35.　以上のような点も念頭に置きながら、以下に示すデータのやり取りのパターンについて理解を深めることも重要である。

(1). コミュニティ内でやり取りする場合

36.　コミュニティ内で合意がなされているトラストフレームワークのもとで、コミュニティの参加者同士がデータのやり取りを行う上では、トラストリスト等の信頼の起点を共有することでトランザクションやメッセージが改ざんされていないことや、相手先の信頼性を構成する要素（例：実在性、資格等）を検証することが可能となる。

37.　トラストリストには、信頼できるアイデンティティとして妥当かどうか検証されたアイデンティティが掲載されており、前述の中カテゴリ相当の項目について、一定の決め事が定められ、その決め事に従ってスクリーニング・認定等がなされることによって担保される。

38.　例えば、移動支援や高齢者見守り等の分野で生活者同士のマッチングによる手助けを促進する共助アプリにおいては、共助アプリ間の決め事をトラストフレームワークによって定め、各共助アプリが共助トラストエコシステム運営というコンソーシアムに参加することで安心してデータのやり取りを行うことができる。

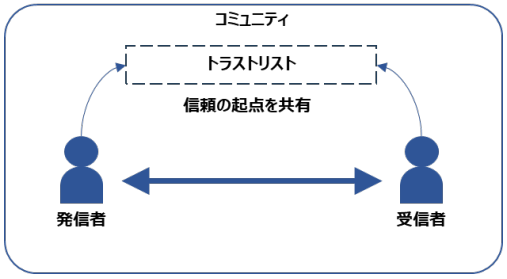

図 5. コミュニティ内でやり取りする場合

(2). コミュニティ間でやり取りする場合

39.　コミュニティ間でやり取りする場合においては、共通して参照するトラストフレームワークの有無やトラストリストの有無によって、パターンが存在する。

（ア）共通して参照するトラストフレームワークのトラストリストを信頼することでやり取り

する場合

40. 異なるコミュニティ間でやり取りする際に、共通して参照が可能となる統一的なトラストフレームワークが整備されている場合がある。

41. その際、各コミュニティが、そのトラストフレームワークに賛同することを表明、規約等に合意、従っていることをスクリーニング・認定等されることで、コミュニティ単位のトラストリストが形成される場合がある。

42. 各コミュニティはそれぞれに参画するアイデンティティのトラストリストを保持するが、コミュニティをまたぐ際にはそのトラストリストは使えない。

43. しかし、相手先のコミュニティと共通して参照するトラストフレームワークのトラストリストを参照することで、相手先コミュニティがそのトラストフレームワークの範囲で信頼することができる。

44. 具体的には、国ごとの業界ルールへの準拠が必要だが、共通ドメインにおいて越境等を想定したデータのやり取りが行われることがある。例えば、国ごとのコミュニティが共通して参照するトラストフレームワークを有する Kantara Initiative や eduGAIN といった団体には、その決め事に準拠している団体のリストが公開されており（日本においては学認がリストに掲載）、掲載された他国とのやり取りで活用することができる。

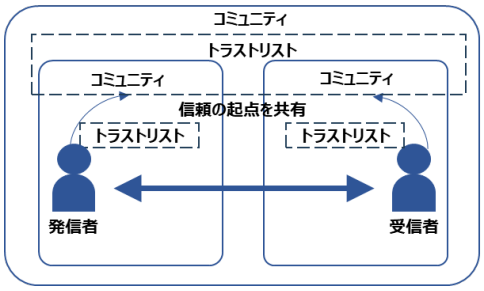

図 6. 共通して参照するトラストフレームワークのトラストリストを信頼することでやり取りする場合

（イ）共通して参照するトラストフレームワークの決め事に準拠した（ただし、そのトラストリストには依拠しない）トラストフレームワークを採用するコミュニティ間でやり取りする場合

45. 異なるコミュニティ間でやり取りする際に、共通して参照が可能となる統一的なトラストフレームワークが整備されている場合があり、各コミュニティは、そのトラストフレームワークに賛同し、規約等に合意、従っていることをコミュニティ毎に表明する場合がある。

46. この際、共通して参照するトラストフレームワークのトラストリストに依拠するだけでは不十分な場合もあるが、相手先のトラストフレームワークの品質（強度）が信頼する上で妥当である場合、相手先のコミュニティを信頼し、データのやり取りを行うこと

ができる。

47. 具体的には、例えば、法人に関する登記の情報に関して、登記・供託オンライン申請システム等を用いて、実在性確認をする際、法人の登記に関するトラストリストが存在し、法人自体が存在していることを検証することはできる。

48. しかしながら、相手先が厳密にどの業種（例：金融機関）に属するかどうかはそのリストでは検証することができない。むしろ、相手先が属する業界に応じた法律（例：銀行法）というトラストフレームワークを外形的に信頼することで、相手先とやり取りすることが可能となる。

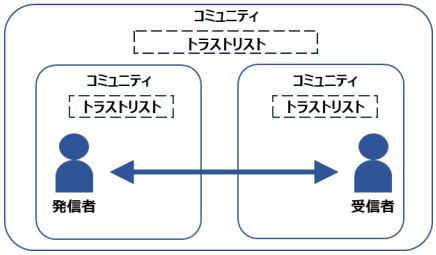

図 7. 共通して参照するトラストフレームワークの決め事に準拠したトラストフレームワーク間でやり取りする場合 [11]

（ウ）共通して参照するトラストフレームワークがない中でコミュニティ間でやり取りする場合

49. 送信元コミュニティと送信先コミュニティが異なる信頼の起点を持ち、かつ共通して参照するトラストフレームワークがない場合においては、相手先のトラストリストを相互承認することでデータのやり取りを行うことが考えられる。

50. 具体的には、PGP のような直接やり取りや特定のプラットフォーム事業者が提供するフェデレーションによる連携が想定される。

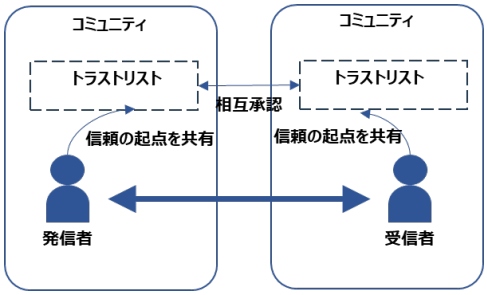

図 8. 異なるコミュニティ間でやり取りする場合

[11] 例えば、受信者が金融機関である場合、発信者は、共通して参照するトラストフレームワークである法人登記に関するトラストリストを確認し、法人の実在性自体を確認する。一方で、受信者が実際に金融機関かどうかは、金融機関のコミュニティで参照している銀行法というトラストフレームワークを外形的に信頼することで、データをやり取りすることが可能となる。